ESD-TR-89-107

Technical Report
851

# Binary Sequences of Arbitrary Length with Near-Ideal Correlation

P.R. Hirschler-Marchand

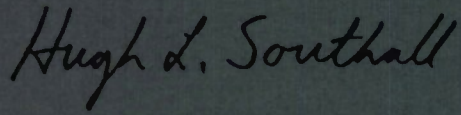
13 June 1989

**Lincoln Laboratory**
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
*LEXINGTON, MASSACHUSETTS*

**Prepared for the Department of the Air Force
under Electronic Systems Division Contract F19628-85-C-0002.**

The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology, with the support of the Department of the Air Force under Contract F19628-85-C-0002.





Hugh L. Southall, Lt. Col., USAF
Chief, ESD Lincoln Laboratory Project Office

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

# BINARY SEQUENCES OF ARBITRARY LENGTH WITH NEAR-IDEAL CORRELATION

*P.R. HIRSCHLER-MARCHAND*
*Group 64*

TECHNICAL REPORT 851

13 JUNE 1989



LEXINGTON MASSACHUSETTS

## ABSTRACT

A new class of binary sequences, called *Mac sequences*, is introduced. These sequences can be designed to have an arbitrary length and near-ideal correlation properties over a specified range around the peak. A systematic algorithm to generate Mac sequences is also presented.

# TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS



## LIST OF TABLES

## ACKNOWLEDGEMENTS

I wish to acknowledge the valuable help of my colleagues in reviewing the manuscript. Particular thanks are due to Dr. A. Sonnenschein and W. C. Cummings whose helpful suggestions and criticism improved the clarity of this report.

# 1. INTRODUCTION

Binary sequences having two-valued correlation are very much sought after. Their applications are found in many areas such as error-correcting codes, synchronization, spread-spectrum communication, time resolution measurements, ranging, picture transmission, acoustics, radar, and antenna design.

Many sequences are known to have two-valued periodic correlation. Perhaps, the most famous of these are *maximum-length* sequences. Maximum-length sequences [1] have two-valued periodic correlations and power spectra. They satisfy linear recursions which are a consequence of Galois field theory [2] and are very easily implemented with linear shift registers. Barker sequences [3] have correlations less than or equal to 1, except at the origin. Twin-prime $(p, p+2)$ sequences [4] have correlation of $p(p+2)$ at the origin and $-1$ elsewhere. Hall sequences [5] and quadratic-residue or Legendre sequences [6] also have the same two-valued periodic correlations and power spectra.

The above sequences have remarkable correlation properties but only come in certain lengths. For instance, maximum-length sequences exist only for periods of length $p^m - 1$. Barker codes are only known for lengths $1, 2, 3, 4, 5, 7, 11$ and 13. Twin-prime sequences only come in lengths $p(p+2)$, where both $p$ and $p+2$ are prime. Hall sequences also are of prime length $p$, with $p$ of the form $4q^2 + 27$. Quadratic residue or Legendre sequences only come in prime lengths $p$ of the form $p = 4q - 1$.

A typical application requires a binary sequence of a specific length and good correlation properties over a given region about the peak. In such cases, it is always possible to use the above sequences in lengths greater than that required by the application, but this is done at the expense of design efficiency or system performance. Also, it is sometimes unnecessary for the ideal correlation properties to extend far beyond the peak of the correlation function. This is the case, for example, of sequences to be used for fine synchronization of communication systems.

Here, the question of interest is whether it is possible to trade a restricted interval of ideal correlation for a greater generality of sequence length. In other words, is it possible to find a class of sequences that exhibit ideal correlation properties over a restricted region around the peak, and whose length can be chosen arbitrarily? As shown in this note, the answer is "yes."

Specifically, this memorandum develops:

- A dense class of binary sequences, called *Mac sequences*, having arbitrary length and ideal correlation properties over a limited range around the peak.
- A general algorithm to construct Mac sequences of any length.

The presentation is organized as follows:

Section 2 recalls the fundamentals of quadratic residues, upon which Mac sequences are based, and Euler's criterion, which will serve in the construction of the desired sequences. The results in this section are well known and can be found in [7]. The following sections contain new material.

Section 3 gives the definition of *Mac sequences* in terms of *core sequences.* A few simple examples are presented to illustrate the definition.

Section 4 establishes the sampling properties of core sequences, as well as the correlation properties of core and Mac sequences. It also addresses the denseness of the set of Mac sequences.

Section 5 discusses computational issues involved with the calculation of quadratic-residue sequences modulo a large prime number, proposes an algorithm to calculate quadratic residues without risk of computer overflow, and develops an easy method to generate Mac sequences. Finally, a long Mac sequence is calculated to illustrate the method, and the resulting binary sequence is shown to have the desired correlation property.

# 2. REVIEW OF QUADRATIC RESIDUES

We now recall some of the properties of quadratic residues and refer the reader to [7] for additional information.

## 2.1 QUADRATIC RESIDUES

**Definition 2.1** *An integer $n$ is a* quadratic residue *modulo a prime number $p$ if the congruence*

$$y^2 \equiv n \pmod{p} \tag{2.1}$$

*has an integer solution $y$. The existence of such a solution is indicated by*

$$n = R \pmod{p} \tag{2.2}$$

*If there is no solution, then $n$ is a* quadratic nonresidue, *and we write*

$$n = N \pmod{p} \tag{2.3}$$

It can be shown [7] that, not counting $n = 0$, there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues.

The properties $R$ and $N$ obey the rules of multiplication of signs, with $R$ corresponding to $+1$ and $N$ to $-1$

$$R \cdot R \equiv R, \quad R \cdot N \equiv N \cdot R \equiv N, \quad N \cdot N \equiv R \tag{2.4}$$

In order to simplify the notation, in this report we will use the Legendre symbol $\left[\frac{n}{p}\right]$, defined as follows:

$$\left[\frac{n}{p}\right] = \begin{cases} 1 & \text{if } n = R \pmod{p} \\ -1 & \text{if } n = N \pmod{p} \\ 0 & \text{if } n \equiv 0 \pmod{p} \end{cases} \tag{2.5}$$

One can define a sequence $\{l_n\}$ as $l_n = \left[\frac{n}{p}\right]$. Such sequences (known as Legendre sequences) are ternary sequences taking values 1, $-1$, and 0 at indices congruent to 0 $(mod\ p)$, and are periodic with period $p$.

## 2.2 EULER'S CRITERION

Euler's criterion is an easy method to check whether a number is a quadratic residue.

**Criterion 2.1** *For a prime $p$ and an integer $n$ such that gcd*[1] $(p, n) = 1$, *$n$ is a quadratic residue modulo $p$ if and only if*

$$n^{(p-1)/2} \equiv 1 \pmod{p} \tag{2.6}$$

*It is a quadratic nonresidue if and only if*

$$n^{(p-1)/2} \equiv -1 \pmod{p} \tag{2.7}$$

*Proof:*

Euler's criterion is based on Fermat's famous theorem [7]:

$$n^{p-1} \equiv 1 \pmod{p}, \quad if \quad gcd\,(p, n) = 1 \tag{2.8}$$

which states that if an integer $n$ and a prime $p$ have no common divisor, then $p$ divides $n^{p-1} - 1$.

Since $n^{p-1} \equiv 1 \pmod{p}$, we have

$$n^{(p-1)/2} \equiv \pm 1 \pmod{p} \tag{2.9}$$

Now, either $n$ is an even power of a primitive root[2] $g$ of 1, or it is an odd power.

If it is an even power, say $n \equiv g^{2m}$, then $g^m$ is a solution to the congruence

$$y^2 = n \pmod{p} \tag{2.10}$$

i.e., $n$ is a quadratic residue modulo $p$.

If it is an odd power, $n$ is a nonresidue because $g^{2m}$ $(m = 1, 2, \ldots)$ generates $(p-1)/2$ quadratic residues, so that the remaining integers must be quadratic nonresidues.

**Definition 2.2** *A* Mac prime *$p$ is a prime number such that $p - 1$ is a nonresidue, hence $p - 1 = N \pmod{p}$.*

By Euler's criterion, a prime $p$ is a Mac prime if and only if $(p - 1)/2$ is odd, since

$$(p-1)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p} \tag{2.11}$$

$$= -1, \quad iff \ (p-1)/2 \ is \ odd \tag{2.12}$$

---

[1] Greatest common divisor

[2] By definition, the successive powers of a primitive root generate a complete residue system, i.e., all integers from 1 to $p - 1$.

# 3. MAC SEQUENCES

We proceed to define the set of Mac sequences and illustrate them with a few examples.

## 3.1 DEFINITION OF MAC SEQUENCES

**Definition 3.1** *Let $p$ be a Mac prime, and let $u, v$ be two arbitrary integers less than $p$. The $(u, p, v)$ Mac sequence $\{b_n\}$ is a binary sequence of length $p+u+v$, defined as follows:*

$$b_n = a_{n-u} \quad for \;\; 0 \leq n < p+u+v \tag{3.1}$$

*where*

$$a_n = \begin{cases} 1 & for\; n \equiv 0 \;\; (mod\; p) \\ \left[\frac{n}{p}\right] & otherwise \end{cases} \tag{3.2}$$

This defines a finite length binary sequence taking values $+1$ and $-1$. The Mac sequence $\{b_n;\; 0 \leq n < p+u+v\}$ can also be expressed as follows:

$$b_n = \begin{cases} \left[\frac{n+p-u}{p}\right] & \text{for } n \text{ satisfying } 0 \leq n < u \\ 1 & \text{for } n = u \\ \left[\frac{n-u}{p}\right] & \text{for } n \text{ satisfying } u < n < u+p \\ 1 & \text{for } n = u+p \\ \left[\frac{n-u-p}{p}\right] & \text{for } n \text{ satisfying } u+p < n < u+p+v \end{cases} \tag{3.3}$$

Note that the sequence $\{a_n\}$ is an infinite binary sequence of period $p$, whereas $\{b_n\}$ is a finite binary sequence of length $p+u+v$. Also, the first $u$ terms and the last $v$ terms of the Mac sequence are the last $v$ terms and the first $u$ terms of the core sequence, respectively. In what follows, the finite subsequence $\{a_n;\; n = 0, \ldots, p-1\}$ of $\{a_n\}$, defined as:

$$a_n = \begin{cases} 1 & \text{for } n = 0 \;\; (mod\; p) \\ \left[\frac{n}{p}\right] & \text{for } n = 1, \ldots, p-1 \end{cases} \tag{3.4}$$

is called the *core sequence* of $\{b_n\}$. It is evident from ( 3.1) that the first $u$ terms of $\{b_n\}$ are the last $u$ terms of $\{a_n\}$, the last $v$ terms of $\{b_n\}$ are the first $v$ terms of $\{a_n\}$, and that the center portion of the Mac sequence is the core sequence. The first $u$ terms and last $v$ terms of the Mac sequence $\{b_n\}$ will be called the *u-term* and *v-term extensions.*

## 3.2 EXAMPLES OF MAC SEQUENCES

### 3.2.1 Example 1: The $(3, 7, 2)$ Mac Sequence

The $(3, 7, 2)$ Mac sequence where $p = 7,\ u = 3,\ v = 2$, is generated from the core sequence $\{a_n; n = 0, \ldots, p-1\}$. For $p = 7$, the quadratic residues are $1, 2, 4$, and the sequence $\{a_n; n = 0, \ldots, 6\}$ is

$$1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1$$

The $u$-term and $v$-term extensions are $1 \ -1 \ -1$ and $1\ 1$, respectively. This provides the resulting (3,7,2) Mac sequence $\{b_n\}$

$$1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1$$

### 3.2.2 Example 2: The $(5, 47, 4)$ Mac Sequence

In a similar fashion, for $p = 47$, the quadratic residues are

$$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 6 & 7 & 8 & 9 & 12 & 14 & 16 & 17 \\ 18 & 21 & 24 & 25 & 27 & 28 & 32 & 34 & 36 & 37 & 42 & \end{array}$$

Thus, the core sequence, $\{a_n; n = 0, \ldots, 46\}$ is

$$\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & \end{array}$$

and the $u$-term and $v$-term extensions are $1 \ -1 \ -1 \ -1 \ -1$ and $1\ 1\ 1\ 1$, respectively.

The $(5, 47, 4)$ Mac sequence is, therefore, equal to

$$\begin{array}{cccccccccccc} 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & & & & \end{array}$$

# 4. PROPERTIES OF MAC SEQUENCES

We now establish several pertinent properties of the core and Mac sequences.

## 4.1 DECIMATION PROPERTY

**Property 4.1** *The core sequences* $\{a_n\}$ *defined by equation ( 3.4) reproduce themselves by decimating with a quadratic residue, i.e., if* $m$ *is a quadratic residue* $(mod\, p)$, *then* $a_{mn} = a_n$.

*Proof:*

From equations ( 2.4) and ( 2.5),

$$a_{mn} = \left[\frac{mn}{p}\right] = \left[\frac{m}{p}\right]\left[\frac{n}{p}\right] = \left[\frac{n}{p}\right] = a_n \tag{4.1}$$

since $\left[\frac{m}{p}\right] = 1$.

## 4.2 BACKWARD RUNNING PROPERTY

By similar reasoning, we have the conjugate property:

**Property 4.2** *If* $m$ *is a quadratic nonresidue, then* $a_{mn} = -a_n$.

In other words, core sequences will reproduce themselves by decimation, except perhaps for the sign.

**Corollary 4.1** *At the exclusion of the first element (corresponding to* $a_0 = 1$*), the core sequence is antisymmetric, i.e.,*

$$a_{-i} = -a_i \quad for\ i = 1, 2, \ldots, p-1 \tag{4.2}$$

This results from the fact that $-1$ is a quadratic nonresidue modulo any prime $p$.

## 4.3 CORRELATION OF CORE SEQUENCES

The cyclic autocorrelation coefficients $K(n)$ of the core sequence $\{a_n\}$ are defined for all values of $n$ as follows:

$$K(n) = \sum_{k=0}^{p-1} a_k a_{k+n} \tag{4.3}$$

and have the following property.

**Property 4.3** *The cyclic autocorrelation coefficients $K(n)$ of the sequence $\{a_n\}$ are two-valued, i.e.,*

$$K(n) = \begin{cases} p & for\ n = 0 \\ -1 & otherwise \end{cases} \tag{4.4}$$

*Proof:*

For $n = 0$, the coefficient $K(n)$ is equal to

$$\sum_{k=0}^{p-1} a_k a_k = \sum_{k=0}^{p-1} 1 = p \tag{4.5}$$

and, thus,

$$K(n) = p \ \ for\ n = 0 \tag{4.6}$$

For $n \neq 0$, one can write

$$\sum_{k=0}^{p-1} a_k a_{k+n} = \sum_{k=0}^{p-1} \left[\frac{k}{p}\right]\left[\frac{k+n}{p}\right] = \sum_{k=0}^{p-1} \left[\frac{k(k+n)}{p}\right] \tag{4.7}$$

Multiplying each Legendre symbol in the last sum by $[\frac{q^2}{p}] = 1$, where $q$ is chosen[1] so that $qn \equiv 1 \ (mod\ p)$, the above sum can be rewritten as

$$\sum_{k=0}^{p-1} a_k a_{k+n} = \sum_{k=0}^{p-1} \left[\frac{qk}{p}\right]\left[\frac{q(k+n)}{p}\right] = \sum_{k'=0}^{p-1} \left[\frac{k'(k'+1)}{p}\right] = c \tag{4.8}$$

where $c$ is now a constant.

Consequently, the cyclic autocorrelation coefficient $K(n)$ is equal to

$$K(n) = \begin{cases} c & \text{for } n \not\equiv 0 \ (mod\ p) \\ p & \text{for } n \equiv 0 \ (mod\ p) \end{cases} \tag{4.9}$$

The constant $c$ is now obtained as follows:

[1] $q$ is simply the inverse of $n$ modulo $p$.

$$\sum_{n=0}^{p-1} K(n) = \sum_{k=0}^{p-1} a_k(a_k + \cdots + a_{k+p-1}) = \sum_{k-0}^{p-1} a_k = 1 \tag{4.10}$$

since, by virtue of the sequence's antisymmetric property, any successive $p$ elements of a core sequence add up to 1. Also, from Equation ( 4.9),

$$\sum_{n=0}^{p-1} K(n) = K(0) + \sum_{n=1}^{p-1} K(n) = p + (p-1)c \tag{4.11}$$

From Equations ( 4.10) and ( 4.11), we conclude that $c = -1$, i.e.,

$$K(n) = \begin{cases} p & \text{for } n \equiv 0 \pmod{p} \\ -1 & \text{for } n \not\equiv 0 \pmod{p} \end{cases} \tag{4.12}$$

This completes the proof of Equation ( 4.3).

## 4.4 CORRELATION OF MAC SEQUENCES

The cross correlation $C(n)$ of the $(u, p, v)$ Mac sequence $\{b_n\}$ and its corresponding core sequence $\{a_n\}$ is defined as follows:

$$C(n) = \sum_{k=0}^{p-1} a_k b_{k+n} \quad for\ 0 \leq n < u + v \tag{4.13}$$

The offset $n$ can be interpreted as the amount by which the lead term of the core sequence is shifted to the right, relative to the lead term of the Mac sequence.

**Property 4.4** *The cross-correlation* $\{C(n),\ 0 \leq n \leq u+v\}$ *of a* $(u, p, v)$ *Mac sequence satisfies:*

$$C(n) = \begin{cases} p & for\ n = u \\ -1 & for\ 0 \leq n \leq u + v\ and\ n \neq u \end{cases} \tag{4.14}$$

In other words, the correlation exhibits a floor at $-1$ on either side of a peak of size $p$. This floor extends to $u$ to the left of the peak, and $v$ to the right of the peak.

*Proof:*

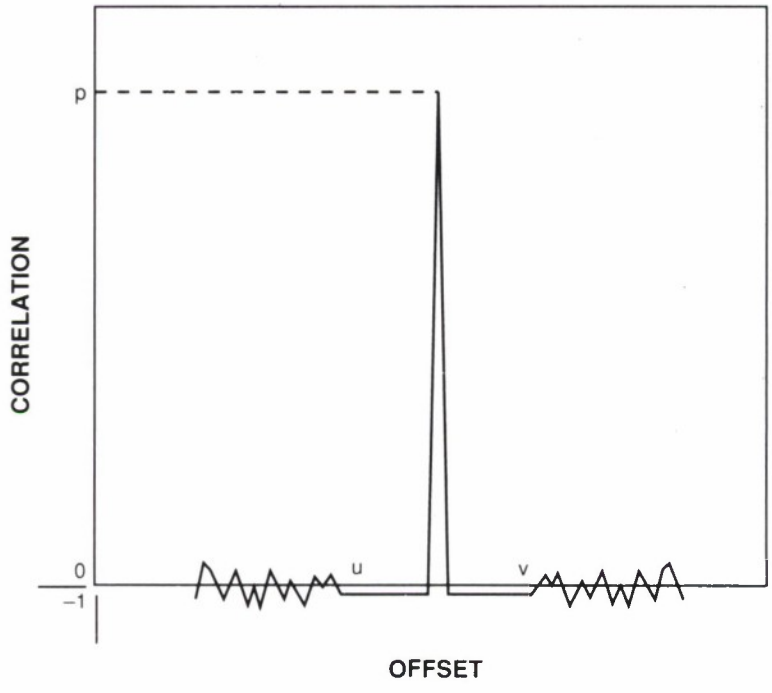
First of all, for $n = u$, the coefficient $C(u)$ is equal to $p$, since

$$\begin{aligned} C(u) &= a_0 b_u + a_1 b_{u+1} + \cdots + a_{p-1} b_{u+p-1} \\ &= a_0 a_0 + a_1 a_1 + \cdots + a_{p-1} a_{p-1} \\ &= K(0) = p \end{aligned} \tag{4.15}$$

For $0 \leq n \leq u+v$ *and* $n \neq u$, we have, using property ( 4.3):

$$\begin{aligned} C(n) &= a_0 b_n + a_1 b_{n+1} + \cdots + a_{p-1} b_{n+p-1} \\ &= a_0 a_{n-u} + a_1 a_{n-u+1} + \cdots + a_{p-1} a_{n-u+p-1} \\ &= K(n-u) \;=\; -1 \end{aligned} \tag{4.16}$$

This completes the proof.




121751-1

*Figure 4-1. Generic correlation of a Mac sequence.*

Property ( 4.4) for Mac sequences results in the generic cross-correlation function shown on Figure 4-1. At the origin, the peak has value $p$, and for the first $u$ ($v$) values to the left (right) of the peak, the correlation is $-1$. Beyond these points, i.e., for $n < 0$ or $n > u+v$, the Mac sequence has to be extended in order to define the correlation. If we assume that the values beyond

the Mac sequence are independent Bernouilli random variables, taking values $\pm 1$ with probability $1/2$, then it can be shown that, averaged over all Mac sequences and random extensions, the correlation coefficient $C(n); n < 0$ has zero mean and standard deviation $\sqrt{\mid n \mid}/2$, and its absolute value is upper bounded by $2 \mid n \mid$. The corresponding statement holds true for $n > u + v$, i.e., the correlation has zero mean, standard deviation $\sqrt{n - (u + v)}/2$, and its absolute value is upper bounded by $2 \mid n - (u + v) \mid$. Consequently, the correlation outside of the $(u, v)$ region grows, on average, at a rate proportional to half the square root of the distance to the correlation floor.

## 4.5 THE CLASS OF MAC SEQUENCES

By definition, Mac sequences are constructed from Mac primes, i.e., prime numbers which satisfy $(p - 1) = N \pmod{p}$. Table 4-1 shows the lists of all Mac primes less than 3000.

The set of Mac sequences is dense, i.e., the existence of many Mac sequences having the same arbitrary length $l = p + u + v$. These sequences differ in the values of $p$, $u$ and $v$, and the value of their correlation coefficients at the origin and beyond the correlation floor. The existence of many Mac sequences of the same length follows from subsequent considerations.

### 4.5.1 Density of Mac Primes

Mac primes constitute a dense set, except perhaps for small values of $p$. Specifically, the prime counting function[2] $\Pi(n)$ is well known, and simple approximations are available [3] such as the "integral logarithm" function, $Li$ [7]:

$$\Pi(n) \approx Li(n) = \int_2^n \frac{dx}{\ln x} \tag{4.17}$$

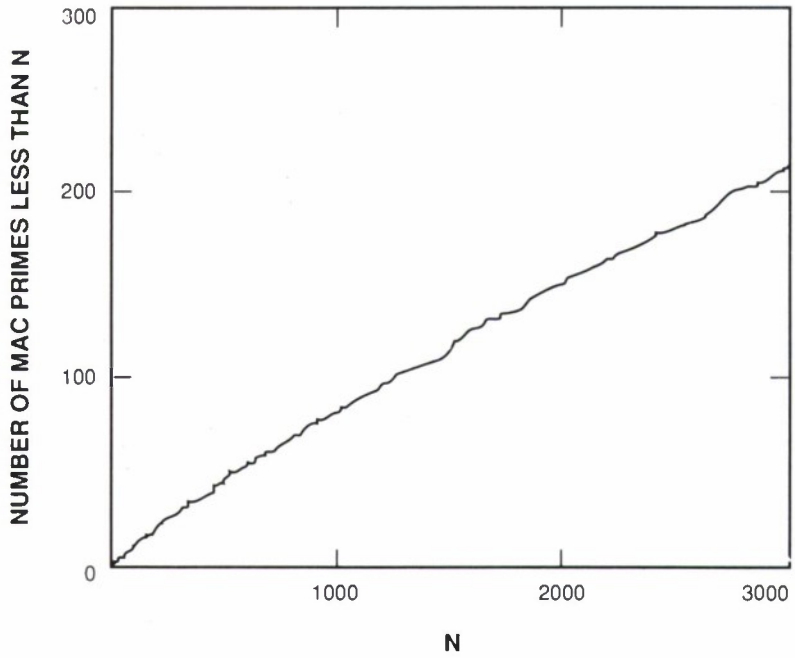
Similarly, we denote by $\Psi(n)$ the Mac prime counting function, i.e., $\Psi(n)$ is the number of Mac primes less than $n$. The average spacing between primes closest to $n$ is approximately $\ln n$, and since there are only half as many Mac primes as there are primes,[4] the average spacing between Mac primes closest to $n$ is approximately $2 \ln n$. Given an *a priori* number $l$ for the length of a Mac sequence, one can always find a Mac prime $p$ within $2 \ln l$ of $l$, on average. For instance, with $l = 1300$, the average spacing between Mac primes closest to 1300 is $2 \ln 1300 \approx 14$. In Table 4-1, the Mac primes closest to 1300 are 1283, 1291, and 1303, with spacings equal to 9 and 12. Figure 4-2 represents the exact Mac prime counting function, $\Psi(n)$, for $1 \leq n \leq 3000$.

---

[2] The number of primes smaller than or equal to $n$.

[3] At least for values of $n$ less than $100,000$.

[4] This results from the fact that the number of primes for which $(p - 1)/2$ is odd or even is about equal, at least for large $p$'s.




121761-2

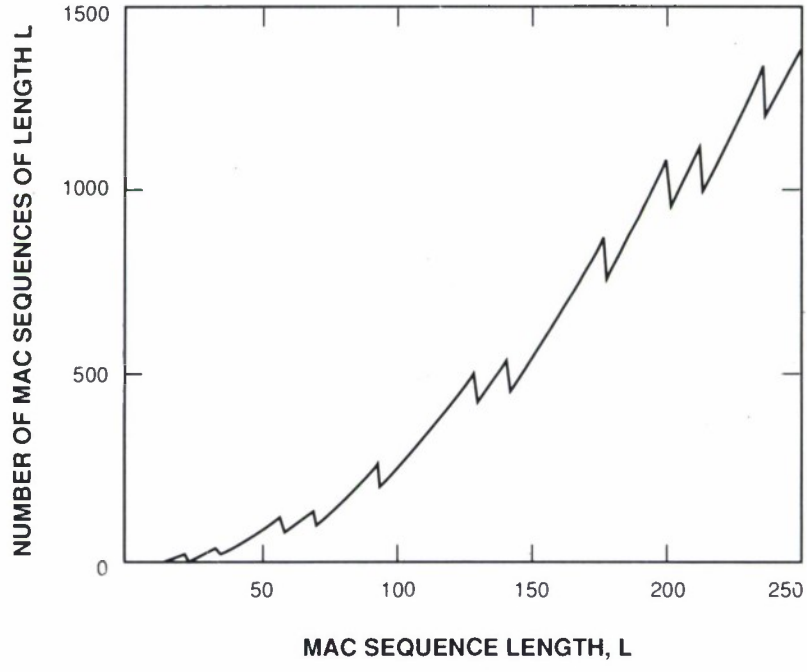
*Figure 4-2. Mac prime counting function.*

### 4.5.2 Number of Mac Sequences of a Given Length

For every Mac prime $p$, there are $(1 + l - p)$ Mac sequences of length $l = p + u + v$, where $u$ and $v$ are less than $p$. They correspond to all possible choices of $u$ and $v$. In addition, for a given $l$, $p$ should be less than $l$ and greater than $l/3$, since $u$ and $v$ are by definition less than $p$. The number of Mac primes $p_j$ between $l$ and $l/3$ is equal to $\Psi(l) - \Psi(l/3)$, where $\Psi$ is the Mac prime counting function defined above. Consequently, the total number $M(l)$ of Mac sequences of length $l$ is equal to:

$$M(l) = \sum_{j=\Psi(l/3)}^{\Psi(l)} (1 + l - p_j) \tag{4.18}$$

The above expression is plotted on Figure 4-3, and shows that there is a large number of Mac sequences of size $l$. A tooth in the curve arises each time the smallest Mac prime between $\Psi(l/3)$ and $\Psi(l)$ is dropped from the sum.




121751-3

*Figure 4-3. Mac sequences of a given length.*

### 4.5.3 Comparison of Mac Sequences of a Given Length

For a given length $l$, the largest Mac prime less than $l$ will lead to the largest correlation peak. At the same time, this will restrict the range $(u, v)$ over which the correlation is $-1$. The choice of the best Mac sequence depends on the application considered. For example, in a communication system in which a Mac sequence is transmitted to a receiving terminal for the purpose of time acquisition, it is desirable to select values of $u$ and $v$ large enough to cover the time uncertainty interval. However, if the Mac sequence is transmitted for the purpose of fine-time tracking, it is preferable to trade-off a larger correlation peak for smaller values of $u$ and $v$, since, in this case, the

time uncertainty interval is much smaller, and a larger correlation peak will provide better tracking in the presence of noise.

TABLE 4-1.

Mac Primes Less Than 3000

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 11 | 19 | 23 | 31 | 43 | 47 | 59 | 67 | 71 | 79 | 83 |
| 103 | 107 | 127 | 131 | 139 | 151 | 163 | 167 | 179 | 191 | 199 | 211 |
| 223 | 227 | 239 | 251 | 263 | 271 | 283 | 307 | 311 | 331 | 347 | 359 |
| 367 | 379 | 383 | 419 | 431 | 439 | 443 | 463 | 467 | 479 | 487 | 491 |
| 499 | 503 | 523 | 547 | 563 | 571 | 587 | 599 | 607 | 619 | 631 | 643 |
| 647 | 659 | 683 | 691 | 719 | 727 | 739 | 743 | 751 | 787 | 811 | 823 |
| 827 | 839 | 859 | 863 | 883 | 887 | 907 | 911 | 919 | 947 | 967 | 971 |
| 983 | 991 | 1019 | 1031 | 1039 | 1051 | 1063 | 1087 | 1091 | 1103 | 1123 | 1151 |
| 1163 | 1171 | 1187 | 1223 | 1231 | 1259 | 1279 | 1283 | 1291 | 1303 | 1307 | 1319 |
| 1327 | 1367 | 1399 | 1423 | 1427 | 1439 | 1447 | 1451 | 1459 | 1471 | 1483 | 1487 |
| 1499 | 1511 | 1523 | 1531 | 1543 | 1559 | 1567 | 1571 | 1579 | 1583 | 1607 | 1619 |
| 1627 | 1663 | 1667 | 1699 | 1723 | 1747 | 1759 | 1783 | 1787 | 1811 | 1823 | 1831 |
| 1847 | 1867 | 1871 | 1879 | 1907 | 1931 | 1951 | 1979 | 1987 | 1999 | 2003 | 2011 |
| 2027 | 2039 | 2063 | 2083 | 2087 | 2099 | 2111 | 2131 | 2143 | 2179 | 2203 | 2207 |
| 2239 | 2243 | 2251 | 2267 | 2287 | 2311 | 2339 | 2347 | 2351 | 2371 | 2383 | 2399 |
| 2411 | 2423 | 2447 | 2459 | 2467 | 2503 | 2531 | 2539 | 2543 | 2551 | 2579 | 2591 |
| 2647 | 2659 | 2663 | 2671 | 2683 | 2687 | 2699 | 2707 | 2711 | 2719 | 2731 | 2767 |
| 2791 | 2803 | 2819 | 2843 | 2851 | 2879 | 2887 | 2903 | 2927 | 2939 | 2963 | |

# 5. COMPUTATIONAL ISSUES

The use of definition ( 2.1) to determine whether or not a number $n$ is a quadratic residue modulo $p$ requires an exhaustive search for a solution to the congruence:

$$y^2 \equiv n \ (mod\, p) \tag{5.1}$$

Euler's criterion, on the other hand, provides a more direct way to determine whether a number $n$ is a quadratic residue or non-residue modulo $p$.

For instance, let $p = 1231$. Determination of, say, element $a_{981}$ in the core sequence requires that one calculate $981^{615}$ $(mod\ 1231)$. Of course, it would be foolish to calculate $981^{615}$, a 1839-digit number, if we are only interested in the remainder modulo 1231. Instead, we need a general algorithm to calculate quadratic residues, and in particular $n^{(p-1)/2}$ $(mod\, p)$.

## 5.1 QUADRATIC RESIDUE ALGORITHM

This algorithm provides a way to calculate, without the risk of computer overflow, the residue modulo any prime $p$ of any number $n$ raised to the power $(p-1)/2$. It can be used equally as well with any power.

**Step 1:**

Find the binary decomposition of $(p-1)/2$:

$$(p-1)/2 \ = \sum_{k=0}^{\lfloor \log_2 (p-1)/2 \rfloor} \alpha_k 2^k \text{ with } \alpha_k = 0 \text{ or } 1 \tag{5.2}$$

where $\lfloor \ \rfloor$ signifies the integer part.

Neglecting the terms with $\alpha_k = 0$ in the above expression, we may write $(p-1)/2$ as a sum of powers of 2:

$$(p-1)/2 = \sum_{m=0}^{M} 2^{c_m} \tag{5.3}$$

Since $(p-1)/2$ is odd, $c_0 = 0$, and therefore,

$$(p-1)/2 = 1 + \sum_{m=1}^{M} 2^{c_m} \tag{5.4}$$

**Step 2:**

Write $n^{(p-1)/2}$ as follows:

$$n^{(p-1)/2} = n \prod_{m=1}^{M} n^{2^{cm}} = n \underbrace{(\ldots(n^2)\ldots)^2}_{c_1 \text{ squarings}} \ldots \underbrace{(\ldots(n^2)\ldots)^2}_{c_M \text{ squarings}} \tag{5.5}$$

and after each squaring and product, reduce the intermediate result modulo $p$.

## 5.2 MAC SEQUENCE GENERATION

The following procedure can now be used to generate a Mac sequence of any length, $l$:

1. *Selection of $p, u, v$:*

   From Table 4-1, select a value of $p$ less than $l$, and greater than $l/3$. As previously mentioned, there are many values of $p$ satisfying this requirement. Select the parameters $u$ and $v$ so that $u + v = l - p$. In the context of an application, restrictions on these parameters will further limit the available choices, as indicated in the previous section.

2. *Generation of the Core Sequence:*

   Using the quadratic residue algorithm described above, generate the core sequence, $\{a_n;\ n = 0, \ldots, p-1\}$ as follows:

$$a_n = \begin{cases} 1 & \text{if } n \equiv 0 \ (mod\ p) \\ 1 & \text{if } n^{(p-1)/2} = 1 \ (mod\ p) \\ -1 & \text{if } n^{(p-1)/2} = -1 \ (mod\ p) \end{cases} \tag{5.6}$$

   Due to the antisymmetry of the core sequence, it is only necessary to calculate the first $(p-1)/2$ terms.

3. *$u$-term and $v$-term Extensions:*

   Define the $u$-term extension as the last $u$ terms of the core sequence, and the $v$-term extension as the first $v$ terms of the core sequence.

4. *Generation of the Mac Sequence:*

   Prefix the $u$-term extension to the core sequence so that it becomes the header of the Mac sequence. Similarly, append the $v$-term extension to the core sequence so that it becomes the tail of the Mac sequence. This will result in the desired $(u, p, v)$ Mac sequence.

## 5.3 EXAMPLE OF A MAC SEQUENCE OF LENGTH 1300

To illustrate the method, we selected an arbitrary number, 1300, and constructed a Mac sequence of length $l = 1300$. Note that there are many Mac sequences of length 1300, as previously indicated. We first select, from Table 4-1, a value of $p$ less than $l = 1300$ and greater than $l/3$, say, $p = 1231$ . The values $u = 35$, and $v = 34$ were selected so as to satisfy $p + u + v = 1300$. The core sequence was generated using a computer program which uses Euler's criterion, the quadratic residue algorithm previously described, and exploits the antisymmetric property of the sequence. The core sequence is shown in Table 5-1. It is now simple to see from Table 5-1 that the $u$-term and $v$-term extensions are as shown in Tables 5-2 and 5-3, respectively. The final Mac sequence of length 1300 results from the concatenation of the $u$-term extension, the core sequence, and the $v$-term extension, in that order. This sequence is shown in Table 5-4

## 5.4 CALCULATED CORRELATION

In Section 4, we proved that the cross-correlation coefficients between the Mac sequence and its core sequence satisfy Equation ( 4.14). The cross-correlation function of the above $(35, 1231, 34)$ Mac sequence was calculated on a computer, and is shown in Figure 5-1 for offsets between $-100$ and $+100$. It satisfies, as expected, the desired two-valued correlation property for Mac sequences.

TABLE 5-1.

Core Sequence of Length 1231

```
1 1 1 -1 1 1 -1 1 1 1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 -1 1 1 -1 1 1 -1
-1 1 1 1 1 -1 1 1 -1 1 1 1 -1 -1 -1 1 1 1 1 -1 -1 1 1 -1 1 -1 -1 -1 1 1 1 1 -1
-1 -1 1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 1 -1 -1
 1 1 1 1 1 -1 1 -1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 1 1 -1 1
-1 1 -1 -1 1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 -1 -1 1 1 -1 1 1 -1 1 1 -1 1 -1 1 1 -1
 1 -1 1 -1 -1 -1 -1 1 -1 1 1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 -1 -1 -1 -1 1 -1 -1
-1 -1 -1 1 1 1 1 1 1 1 1 1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 -1 1 1 -1 -1 -1 1 1
-1 1 -1 -1 -1 -1 1 1 1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 1
-1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 1 1 1 1 1 1 -1 1 -1 -1 -1 1 1 1
1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 1 1 1 1 -1 -1 1 1 -1 1 1 1 1 -1
-1 -1 1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 -1 -1 1 -1 1 1
1 -1 -1 1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 -1 1 -1 -1 -1 1 -1 1 1 -1 1 -1 1 -1
-1 1 -1 1 -1 1 1 1 1 -1 1 1 1 -1 1 1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1
 -1 -1 -1 -1 -1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1
-1 1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 -1 -1 -1 -1 1 1 1 -1 -1 -1 1
-1 1 -1 1 1 1 -1 -1 1 1 -1 -1 -1 1 1 1 1 -1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 -
1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 -1 1 -1 -1
 1 -1 -1 -1 -1 -1 1 -1 1 1 1 -1 1 -1 1 -1 1 1 1 1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1
1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 1 -1 -1 1 -1 -1 1 -1 1 1
 -1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 1 1 -1 -1 1 -1 -1 1 -1 1 1 -1 1 1 -1 1 1
 1 -1 1 1 -1 1 -1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 -1
-1 1 -1 -1 -1 -1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 1 1 1 1 -1 1 1 -1 1 1 1 -1 -1 -1
-1 1 1 -1 1 1 1 1 1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 1 1 -1 -1 1 1 -1 -1
1 -1 1 -1 -1 -1 1 1 1 -1 -1 1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 -1 -1 1 1 1 1 -1
-1 -1 1 -1 -1 1 1 1 -1 1 1 1 -1 -1 1 1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 1 1 1
-1 -1 1 1 -1 1 -1 1 -1 1 1 1 1 1 1 1 -1 1 -1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1
-1 -1 -1 1 -1 -1 -1 1 -1 -1 -1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 1 1 1 -1
1 1 -1 -1 1 -1 -1 1 -1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 1 -1 -1 -1
-1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1
-1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 1 1 -1
1 -1 -1 -1 -1 -1 -1 -1 1 1 -1 1 1 1 -1 -1 1 1 1 1 -1 -1 -1 1 1 -1 -1 1 1 1 -1 1
-1 -1 -1 -1 1 -1 -1 1 1 1 -1 1 1 1 1 -1 1 1 1 -1 -1 1 -1 1 1 1 1 -1 -1 1 1 1 -1
1 -1 1 -1 -1 -1 1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1
1 1 -1 1 -1 -1 -1 -1 -1 1 -1 -1 -1 1 1 -1 -1 1 -1 1 1 1 1 -1 1 -1 1 -1 -1 1 -1
1 -1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 -1 -1 -1 1 1 1 -1 1 1 -1 1 -1 1 -1
 -1 -1 1 1 -1 1 1 1 -1 -1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 -1 -1 -1 -1 1 1 -1 1
 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 1 -1 -1 -1
-1 1 1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 1 1 1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 -1 1 1 -1
 -1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 -1 1
-1 -1
```

TABLE 5-2.

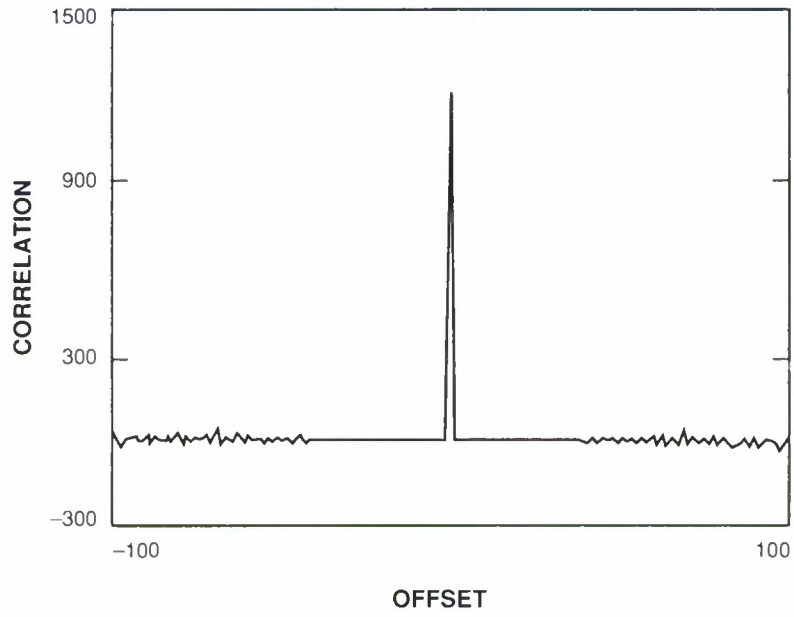
$U$-term Extension of the $(35, 1231, 34)$ Mac Sequence

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | $1$ | $1$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ | $1$ | $1$ | $-1$ | $1$ | $-1$ | $-1$ | $-1$ |
| $1$ | $-1$ | $1$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ | |

TABLE 5-3.

$V$-term Extension of the $(35, 1231, 34)$ Mac Sequence

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $1$ | $-1$ | $1$ | $1$ | $-1$ | $1$ | $1$ | $1$ | $1$ | $1$ | $-1$ | $1$ | $1$ | $-1$ | $1$ | $-1$ |
| $1$ | $1$ | $1$ | $-1$ | $1$ | $-1$ | $-1$ | $1$ | $1$ | $-1$ | $1$ | $1$ | $-1$ | $1$ | $1$ | $-1$ | | |




121751-4

*Figure 5-1. Cross-correlation of the $(35, 1231, 34)$ Mac sequence.*

TABLE 5-4.

(35, 1231, 34) Mac Sequence

```
-1 1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 -1 1
-1 -1 1 -1 -1 1 1 1 -1 1 1 -1 1 1 1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 -1
1 1 -1 1 1 -1 -1 1 1 1 1 -1 1 1 -1 1 1 1 -1 -1 -1 1 1 1 1 -1 -1 1 1 -1 1 -1 -1
-1 1 1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 -1 1 1 -1
-1 -1 1 -1 -1 1 1 1 1 1 -1 1 -1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 -1 -1
 1 1 1 -1 1 -1 1 -1 -1 1 -1 -1 1 1 1 1 1 -1 1 1 1 -1 -1 1 1 -1 1 1 -1 1 1 -1
 1 -1 1 1 -1 1 -1 1 -1 -1 -1 -1 1 -1 1 1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 -1 -1 -1
 -1 1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 -1 1 1
-1 -1 -1 1 1 -1 1 -1 -1 -1 -1 1 1 1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 1 -1 1 1 1 1 -1
 1 -1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 1 1 1 1 1 1 -1 1 -1
 -1 -1 1 1 1 1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 1 1 1 1 -1 -1 1 1
-1 1 1 1 1 -1 -1 -1 1 1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1
-1 -1 1 -1 1 1 1 -1 -1 1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 -1 1 -1 -1 -1 1 -1 -1
1 1 -1 1 -1 1 -1 1 -1 1 -1 1 1 1 1 -1 1 1 1 -1 1 1 1 1 1 1 1 1 1 1 -1 -1 -1
-1 -1 1 -1 1 -1 -1 -1 -1 -1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1
 -1 -1 -1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 -1 1 1 1 -1 -1 -1 -1 1
1 1 -1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 1 -1 -1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 1 1
-1 -1 -1 -1 1 -1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 1 -1 -1 1 1 1 1
-1 -1 -1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 -1 1 -1 1 -1 1 1 1 1 -1 1 1 -1 -1
1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 1 -1 -1
1 -1 -1 1 -1 1 1 -1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 1 1 -1 -1 1 -1 -1 1 -1 1
 1 -1 1 1 -1 1 1 1 -1 1 1 -1 1 -1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 -1 -1 1
-1 1 -1 1 1 -1 -1 1 -1 -1 -1 -1 1 -1 1 1 -1 1 -1 -1 1 -1 1 1 1 1 1 -1 1 1 -1 1
 1 1 -1 -1 -1 -1 1 1 -1 1 1 1 1 1 1 -1 -1 -1 -1 -1 1 1 1 1 -1 1 -1 1 1 1 1 1 -1
 -1 1 1 -1 -1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 -1
-1 -1 -1 -1 -1 -1 -1 -1 1 -1 -1 -1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 -1 1
1 -1 1 1 1 -1 1 1 -1 -1 1 -1 -1 1 -1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1
-1 1 -1 -1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 -1 -1 1 -1 1 1 1 -1 -1 -1 -1
 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 -1 -1
-1 1 1 1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 -1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 1 1 -1
-1 1 1 -1 1 -1 -1 -1 -1 1 -1 1 1 -1 1 1 1 1 -1 1 1 -1 -1 -1 1 1 1 1 -1 1 -1 -1
1 1 1 -1 -1 1 -1 1 -1 -1 -1 1 1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1
 1 1 -1 1 1 1 1 -1 1 -1 -1 -1 -1 -1 1 -1 -1 -1 1 1 -1 -1 1 -1 1 1 1 1 -1 1 -1 1
 -1 -1 1 -1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 -1 -1 -1 -1 1 1 1 -1 1 1
-1 1 -1 1 -1 -1 -1 1 1 -1 1 1 1 -1 -1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 -1 -1 -1
 1 1 1 -1 1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 -1 -1 1 1
 1 -1 -1 -1 -1 1 1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 1 -1 -1 -1 1 -1 -1 1 -1 -1
-1 -1 1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 -1
 1 -1 -1 1 -1 -1 1 1 1 -1 1 1 -1 1 1 1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1
-1 1 1 -1 1 1 -1
```

## 6. CONCLUSION

A new class of binary sequences, called Mac sequences, has been constructed. These Mac sequences exhibit near-ideal correlation properties and can have arbitrary length. Specifically, the $(u, p, v)$ Mac sequence has length $p + u + v$, a correlation with a peak value of $p$ at the origin, and equal to $-1$ over the region $-u, +v$ around the peak. Beyond this region, the correlation is well behaved. An algorithm is given which allows easy generation of Mac sequences with the help of a small computer. The availability of binary sequences of arbitrary length with near-ideal correlation properties allows the Mac sequences to be used in a large variety of applications.

## REFERENCES


1. S. W. Golomb, *Shift Register Sequences* (Holden-Day, San Francisco, 1967).

2. E. R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, New-York, 1968).

3. R. H. Barker, "Group Synchronizing of Binary Digital Systems," in *Communication Theory*, W. Jackson, ed. (Academic Press, New York, 1953.)

4. A. Brauer, "On a New Class of Hadamard Determinants," *Mathematische Zeitschrift*, **58**, (1953).

5. M. Hall, Jr., "A Survey of difference Sets,"Proc. Am. Math. Soc. , **7**, pp. 975-986 (1956).

6. R. E. Paley, "On Orthogonal Matrices,"J. Math. Phys. , **12**, 1933.

7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th Edition (Clarendon, Oxford, 1984).

8. M. R. Schroeder, *Number Theory in Science and Communication*, Second Enlarged Edition (Springer-Verlag, 1985).

9. M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions* (Dover Publications, Inc., New York).

# REPORT DOCUMENTATION PAGE

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>Unclassified | 1b. RESTRICTIVE MARKINGS |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>Approved for public release; distribution is unlimited. |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S)<br>Technical Report 851 | 5. MONITORING ORGANIZATION REPORT NUMBER(S)<br>ESD-TR-89-107 |
| 6a. NAME OF PERFORMING ORGANIZATION<br>Lincoln Laboratory, MIT<br>6b. OFFICE SYMBOL *(If applicable)* | 7a. NAME OF MONITORING ORGANIZATION<br>Electronic Systems Division |
| 6c. ADDRESS *(City, State, and Zip Code)*<br>P.O. Box 73<br>Lexington, MA 02173-0073 | 7b. ADDRESS *(City, State, and Zip Code)*<br>Hanscom AFB, MA 01731 |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>HQ AF Systems Command<br>8b. OFFICE SYMBOL *(If applicable)*<br>AFSC/XTKT | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER<br>F19628-85-C-0002 |
| 8c. ADDRESS *(City, State, and Zip Code)*<br>Andrews AFB<br>Washington, DC 20334-5000 | 10. SOURCE OF FUNDING NUMBERS<br>PROGRAM ELEMENT NO. 33110F, 33603F; PROJECT NO. 370; TASK NO.; WORK UNIT ACCESSION NO. |
| 11. TITLE *(Include Security Classification)*<br>Binary Sequences of Arbitrary Length with Near-Ideal Correlation | |
| 12. PERSONAL AUTHOR(S)<br>Patrick R. Hirschler-Marchand | |
| 13a. TYPE OF REPORT<br>Technical Report<br>13b. TIME COVERED<br>FROM _____ TO _____ | 14. DATE OF REPORT *(Year, Month, Day)*<br>13 June 1989<br>15. PAGE COUNT<br>36 |
| 16. SUPPLEMENTARY NOTATION | |

| 17. COSATI CODES | | | 18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)* |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | binary sequences, ideal correlation, acquisition, synchronization, prime numbers, quadratic residues, legendre sequences, two-valued correlation |
| | | | |
| | | | |

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

A new class of binary sequences, called Mac sequences, is introduced. These sequences can be designed to have an arbitrary length and near-ideal correlation properties over a specified range around the peak. A systematic algorithm to generate Mac sequences is also presented.

| | |
|---|---|
| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT<br>☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS | 21. ABSTRACT SECURITY CLASSIFICATION<br>Unclassified |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>Lt. Col. Hugh L. Southall, USAF | 22b. TELEPHONE *(Include Area Code)*<br>(617) 981-2330<br>22c. OFFICE SYMBOL<br>ESD/TML |